Notice of Allowability	**Application No.** 09/885,234	**Applicant(s)** CORMACK ET AL.	
	Examiner Samson B. Lemma	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--
All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amedment filed on 10/26/2006*.

2. ☒ The allowed claim(s) is/are *1-4, 6, 10-15, 19-22, 24 and 29*.

3. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) □ All b) □ Some* c) □ None of the:
   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) □ hereto or 2) □ to Paper No./Mail Date _____.
   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)
1. □ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. □ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

DETAILED ACTION

1. This is in reply to amendment after non-final office action, filed **on October 26, 2006**. Claims 5, 7-9, 16-18, 23, 25-28 and 30-31 are canceled. Thus **claims 1-4, 6, 10-15, 19-22, 24 and 29** are pending/examined. Claims 1-3, 6, 10-12, 15, 19-22 and 24 are amended.

Allowable Subject Matter

2. **Claims 1-4, 6, 10-15, 19-22, 24 and 29** are allowed.

3. The following is an examiner's statement of reasons for allowance:

4. **Independent Claims 1, 10 and 19 are allowed for** the following reasons.

5. The combination of the references on the record, namely Kathrow and Pereira discloses each and every limitation of the independent claims, before the claims were amended. For instance, referring to the independent claims 1, 10 and 19, the reference on the record namely **Kathrow** discloses a method to detect tampering with registry settings in a computer comprising:

- **Generating a user identity value [hash Value of the user Password] associated with a user identity**; (In Microsoft operating system, in the process of authentication, generation of a user identity value or the hash value of the user password is inherently included. For NT, user enters their password and the clients hashes the user's password, and generates the hash value or the user identity value and encrypts the server's challenge with this hash and sends two responses to the server: One response uses the LAN Manager hash and another response uses the stronger NT hash. The server then compares the client's response hash with the client's hash in the SAM Registry hive.)(For the source/explanation that the examiner used, see reference U, page 2, second paragraph)

- **the user identity value is generated by a one-way function [hash Value of the user Password meets the limitation of a one-way function]** (In Microsoft operating system, in the process of authentication, generation of a user identity value or the hash value of the user password is inherently included. For NT, user enters their password and the clients hashes the user's password, and generates the hash value or the user identity value and encrypts the server's challenge with this hash and sends two responses to the server: One response uses the LAN Manager hash and another response uses the stronger NT hash. The server then compares the client's response hash with the client's hash in the SAM Registry hive.)(For the source/explanation that the examiner used, see reference U, page 2, second paragraph)

- **Storing the user identity value [hash value of the user password]**; (Storing the **client's hash** or **the user identity value** or **the hash value of the user password**, in the SAM Registry as explained above for the purpose of authentication is inherently included in the Microsoft operating system, NT) (For the explanation/source that the examiner used See reference U, page 2, second paragraph)

Furthermore **Kathrow** discloses

- **Generating a registry security value [Fingerprint of the registry file/s which includes hash value of the Windows registry file/s] associated with a system registry**; [column 5, lines 11-25; column 4, lines 26-column 5, line 25; figure 2, ref. Num "222" and "232"]

- **Storing the registry security value**; [Column 5, lines 11-26; figure 2, ref. Num "232"] (content storage stores the fingerprint of the file shown on figure 2, ref. Num "232") and

- **Authenticating by the application program the system registry after reading the system registry**.(As explained in the disclosure and on the dependent claim 5, this limitation **comprises**

- **Generating a new registry security value [Fingerprint of the registry file/s which includes hash value of the Windows registry file/s]**; [Column 5, lines 41-62; figure 2, ref. Num "234"] (The new registry finger print is generated and stored on storage shown on figure 2, ref. Num "234"]

- **Comparing the new registry security value with the stored registry security value**; [Column 6, lines 20-21; column 7, lines 1-6; figure 2, ref. Num "242"] and **allowing processing to continue if the new registry security value is equal to the stored registry security value**. [Column 6, lines 32-36; column 10, lines 38-43] (The processing will not be allowed to continue if the new registry security value is not equal with the stored security value. If this is the case, that is if they are found to be different, then the comparison result will be reported.)

Kathrow does not explicitly disclose

A user identity value associated with a user identity authorized to change a system registry of the computer is generated by an application program running in the computer and

The generated registry security value which associated with system registry is generated by the application program.

However, in the field of endeavor **Pereira**, discloses

The access control program may use an application program interface (API) to modify the registry system file in accordance with the restricted list files generated by the access control program. [Column 10, lines 29-33 and column 10, line 1-column 11, line 10]. This meets the limitation of A user identity value associated with a user identity authorized to change a system registry of the computer is generated by an application program running in the computer and the generated registry security value which associated with system registry is generated by the application program.

Furthermore **Pereira** discloses detecting an attempt to change a system registry;[column 4, lines 49-54; column 4, lines 40-44; column 4, lines 49-51 column 10, lines 20-21] and generating a user identity value associated with the user identity;[column 10, lines 20-26] (if the user enters the corresponding password user would be able to define/access resources in the registry)

However, as applicant persuasively argued the reference on the record namely the combination of Kathrow and Pereira does not disclose the following (underlined) limitation recited in the present independent claims, "generating a registry security value associated **each time a system registry setting is changed by an authorized user**;

storing the registry security value;

when reading from the system registry, generating a new registry security value, comparing the new registry, security value with the stored registry security value and allowing processing to continue if the new registry security value is equal to the stored registry security value

when monitoring the system registry for attempts to change the system registry, prompting for user identity information and generating a new user identity value associated with a new user identity seeking access to the system registry and comparing the new user identity value to the stored user identity value; " as recited in the respective independent claim.

None of the prior art of record taken singularly of in combination teaches a method to detect tampering with registry settings in a computer with the with this particular functional limitation recited above together with the other limitation recited in respective independent clams. For this reason, independent claims **1, 10 and 19** are found to be novel and are allowed.

Support for the above amendment is found on the applicant disclosure on paragraph 0013-0018 and figure 2 and 3.

6. The dependent **claims** which are dependent on the above **independent claims 1, 10 and 19** being further limiting to the independent claim, definite and enabled by the specification are also allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
11/10/2006

GILBERTO BARRON Jr
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100